Towards new data protection principles in a new ICT environment

Dinant, Jean-Marc; Poullet, Yves

Published in:
Revista de Internet, derecho y politica

Publication date:
2007

Document Version
Publisher's PDF, also known as Version of record

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monograph "III Conference on Internet, Law and Politics (ILP). New outlooks"

ARTICLE

Towards new Data Protection Principles in a new ICT environment

Yves Poullet
with the cooperation of Jean-Marc Dinant

Submission date: May 2007
Acceptation date: May 2007
Published in: September 2007

Abstract
In view of the new transformations of the Internet, among which we can highlight the trend towards previously autonomous network connections and the multifunctionality of telecommunication terminals, which make information systems omnipotent, new principles must be established in order to provide adequate protection for citizens.
Five new principles are proposed: encryption and reversible anonymity; reciprocal benefits, whereby technology also benefits users; improvement of technological solutions that favour or do not work against privacy – as established by the Group from article 29; complete user control over the terminal, so that he or she is fully informed as to the data flow; and the principle whereby users of certain information systems benefit from legislation in defence of consumers and users.
Furthermore, the obligation to comply with personal data protection regulations must be extended to other subjects that do not initially appear to be involved in processing: namely, software and terminal manufacturers. These are obliged to inform users about any risks that they run when using networks, as well as provide access to applications and manufacture products that ensure greater protection of privacy.

Keywords
networking, new data protection principles, liability, software manufacturers, telecommunication terminal manufacturers, information for users

Topic
Data protection

Hacia nuevos principios de protección de datos en un nuevo entorno TIC

Resumen

Ante las nuevas transformaciones de Internet, entre las que podemos destacar la tendencia a la conexión de redes hasta ahora autónomas y la multifuncionalidad de los equipos terminales de telecomunicaciones, que convierten los sistemas de información en omnipresentes, hay que establecer nuevos principios para proteger adecuadamente al ciudadano.

Se proponen cinco nuevos principios. El de encriptación y anonimato reversible; el de beneficios recíprocos, de tal manera que la tecnología también beneficie a los usuarios; el de potenciación de las soluciones tecnológicas que favorezcan o no vayan en contra de la privacidad –tal como establece el Grupo del artículo 29–; el del completo control por parte del usuario del equipo terminal, de modo que éste se mantenga completamente informado de los flujos de datos, y el principio según el cual los usuarios de determinados sistemas de información se beneficien de la legislación sobre defensa de los consumidores y usuarios.

Además, la obligación de cumplimiento de las normas de protección de datos de carácter personal debe hacerse extensiva a otros sujetos que, de entrada, no parecen involucrados en el tratamiento: los fabricantes de software y de terminales. Éstos tienen el deber de informar al usuario de los riesgos que corren al utilizar las redes y de ofrecer acceso a aplicaciones y fabricar productos que garanticen una mayor protección de la privacidad.

Palabras clave

conexión de redes, nuevos principios de protección de datos, responsabilidad, fabricantes de software, fabricantes de terminales de telecomunicaciones, información al usuario

Tema

Protección de datos

Introduction: A new ICT environment

1. Internet and, more broadly, the multiplication of ICT in daily life (GPS, RFID, mobile) have radically modified the environment and created new risks for our privacy considered in a broad sense. The last two decades have seen an incredibly fast succession of an impressive number of innovations and technological trends that have led to the forming of a global telecommunications network. This technological development has taken place on an international level without any government or civic movement playing a decisive role and without the problems of a reduction in privacy brought about by these networks being tackled or resolved from the technical point of view.

2. One might summarise as follows the characteristics of this environment and suggest certain achievements in order to ensure a better protection of citizens, which are becoming more and more "netizens".[1]

The network is **multifunctional** and tends to link together all existing telecommunication networks hitherto kept autonomous. The capacity of the communication infrastructure is growing and one speaks about 10 Kbits/sec.

As regards **the terminal equipment**, one denotes different evolutions; firstly, the terminal equipment which in the eight-

1. For a complete description, read Y. POULLET; J.M. DINANT (Nov. 2004). *Self-determination in an Information Society, Report on the application of Data Protection Principles to the worldwide Telecommunications networks*. Report for the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal Data (T-PD). Strasbourg. Available on the Council of Europe website. The present article is a deeply revised and shorted version of this report.

ies was unifunctional (the voice telephony terminal for the transmission of audio signals, the T.V. for the one-way transmission of images, etc.) is now multifunctional. With my laptop I am able to send mails, watch TV, make transactions and read my newspaper. Another evolution is definitively the fact that they are no longer linked to a fixed place but accompany us in our movements. Their capacity is increasing tremendously under the famous Moore's Law. According to this theory, every eighteen months, the capacity of a terminal might be doubled for the same prize. In other words, after fifteen years the computers' processing and storage capacities are multiplied by one thousand. Concretely, this means that a computer bought in a supermarket undergoes the following evolution:

Year	1987	2005	2020 (x1000)
Processor	8 Mhertz	3 Ghertz (x 375)	3 TeraHz
Memory	640KB	512 MB(x 800)	512 Gbytes
Hard Disk	20 Mbytes	120 Gbytes (x 6000)	120 Terabytes
Phone conn.	10Kb/sec	3 Mb /sec	10 Gb/sec

Finally, one also underlines the trend towards a **miniaturisation** of the terminal thanks to the use of nanotechnology. RFID are tags called "smart dust" and might be embedded in our clothes, in the products we buy in supermarkets, and even in our brain, in order to detect, control and ultimately influence our behaviour.

Through the use of these various terminals, Information systems are **ubiquitous** since they have invaded our environment and all segments of our daily life, both private and professional, and with each passing day it will make further inroads into numerous fields and the objects surrounding us. It multiplies the traces of the ICT services' usages and the possibility for certain data controllers to control the activities of Internet users.

Many activities which in the past were carried out without any telecommunications network will require such networks to be used in the future. It is not at all unreasonable to think that, in a few years time, most refrigerators will be equipped with intelligent components which will know exactly what food is stored in the refrigerator and when it will be past its sell-by date (thanks to RFID chips). These "intelligent" refrigerators would even be able to take the initiative of displaying on the family TV set targeted advertisements or indeed of contacting supermarkets to obtain offers or order goods. In general, there is a clear tendency to make the objects surrounding us more intelligent by equipping them with a telecommunications terminal. Intelligent terminals are operating in an **opaque and complex** way.

3. Today, computers make up the vast majority of telecommunications terminals. Being based on computers, these terminals generate, in a manner completely invisible to their users, many tracks of the telecommunications that pass through them. These tracks are either stored within the terminal or sent over the network, usually without informing the user. The technical means placed at the users' disposal are incomplete, too complex and configured by default in a way detrimental to the protection of the web surfers' privacy. Respect for privacy has become an option accessible to people with the time and the knowledge at their disposal. The individual's relationship with the protection of his or her data has itself become an item of personal information that many players want to possess.

Telecommunications terminals incorporate various technical identifiers that make it possible to "track" the behaviour of the individual on the network. Most industry players do not consider this tracking process a violation of the privacy of the individual if the latter cannot be identified by a contact point. Cookie technology enables a third-party web site, by default, surreptitiously to insert its own identifier into the terminal on a permanent basis so as to be able to track an individual's behaviour on the internet.

4. Telecommunications protocols and the functioning of the terminals do not include data protection as a key requirement but as an option generally left to the discretion of manufacturers of the hardware and software that incorporates these standards. **Certain opinions expressed recently by article 29 WG have argued that the principle enacted by Recital 2 of the E.U Directive 95/46 on Data Protection, which clearly asserts that**

technology must be at the benefit of the individuals and society, might be considered as a justification for imposing on manufacturers of terminal equipment (including software elements incorporated into the terminal) certain obligations aimed at the transparency of their operation and preventing the unfair or illicit use of personal data associated with the connecting to and communicating with the network. It should be noted that these manufacturers are not covered as such by the present directive since they are not controllers of a file. However, as the design of the equipment they supply authorises many processing operations, certain security responsibilities should be imposed on them so as to prevent those operations that could be carried out by third parties in an unfair or illicit manner, and they should be required to ensure transparency since the user of the equipment must be able to exercise a certain amount of control over the data flows generated by its use.

5. Finally, we might point out the global character of the Internet. Due to the global nature of the modern networks and the absence of frontiers as regards infrastructures, the processing operated by persons located outside of the national borders might directly affect our privacy by sending spyware, transmitting data to third parties through invisible hyperlinks or addressing unsolicited mails through the web, etc. The abolition of national borders makes necessary a common approach towards Data Protection principles and their possible enforcement beyond the frontiers. The WSIS has clearly pleaded in favour of an international recognisance of Privacy Protection.

Some new principles to promote informational self-determination in the new technological environment

6. Those features that are most characteristic of the electronic communications service environment – growing presence and multifunctionality of electronic communications networks and terminals, their interactivity, the international character of networks, services and equipment producers and the absence of transparency in terminal and network functioning – all increase the risk of infringing individual liberties and human dignity.

To counter these risks, certain new principles must be established if data subjects are to be better protected and have more control over their environment. Such control is essential if those concerned are to exercise effective responsibility for their own protection and be better equipped to exercise proper informational self-determination.

This is a first attempt to outline such principles. It is based on a range of material and we have tried to structure it around five main principles, since at this stage we prefer not to speak of new "rights" for data subjects. Their content and extension should be discussed by the different stakeholders and could then, if appropriate, form the basis for recommendations and other *ad hoc* measures to give them greater force.

a. First principle: The principle of encryption and reversible anonymity

7. Message encryption offers protection against access to the content of communications. The quality varies, as do encryption and de-encryption techniques. Encryption software for installation on internet users' computers (S/MIME or Open PGP protocols) are now available at a reasonable price. Meanwhile, given its ambiguity, the notion of anonymity should perhaps be clarified, and possibly replaced by other terms such as "pseudonymity" or "non-identifiability". What is sought is often not absolute anonymity but rather **the functional non-identifiability of the author of a message vis-à-vis certain persons**.[2] There are many non-binding documents[3] advocating citizens' "right" to anonymity when using new technological services. Recommendation No R (99) 5[4] of the Council of Europe's Committee of Ministers states that "*anonymous access to and use of services, and anonymous means of making payments, are the best protection of privacy*", hence the importance of privacy enhancing techniques already available on the market.

2. See J. GRIJPINK; C. PRIENS (2001). "Digital Anonymity on the Internet: New Rules for Anonymous Electronic Transactions?". *Computer Law & Security Report*. Volume 17, Issue 6, pp. 379-389.
3. See in particular S. RODOTÀ. "Beyond the E.U. Directive: Directions for the Future". In: Y. POULLET, C. de TERWANGNE; P. TURNER (ed.). "Privacy: New Risks and Opportunities". *Cahier du CRID*. Antwerpen: Kluwer. Nº 13, p. 211 ff.

The first principle: that of functional non-identifiability might be expressed as follows: **Those using modern communication techniques must be able to remain unidentifiable by service providers and other third parties intervening during the transmission of the message and by the recipient or recipients of the message, and should have free or reasonably priced access to the means of exercising this option.**[5] **The availability of readily affordable encryption and anonymisation tools and services is a necessary condition for computer internauts' exercising personal responsibility**.

The anonymity or "functional non-identifiability" required is not absolute however. Citizens' right to anonymity has to be set against the higher interests of the state, which may impose restrictions if these are necessary "*to safeguard national security, defence, public security, [and for] the prevention, investigation, detection and prosecution of criminal offences*". Striking a balance between the legitimate monitoring of offences and data protection may be possible through the use of "pseudo identities", which are allocated to individuals by specialist service providers who may be required to reveal a user's real identity, but only in circumstances and following procedures clearly laid down in law.

8. Other consequences might be drawn down from this first principle: so it might include the enforced regulation of terminal equipment, to prevent browser chattering, permit the creation of ephemeral addresses and differentiation of address data according to which third parties will have access to the traffic or localisation data, and the disappearance of global unique identifiers by the introduction of uniform address protocols.

Finally, the status of "anonymisers", on which those who use them place great reliance, should be regulated to offer those concerned certain safeguards regarding the standard of service they provide while ensuring that the state retains the technical means of accessing telecommunications in legally defined circumstances.[6]

b. Second principle: The principle of reciprocal benefits

9. This principle would make it a statutory obligation, wherever possible, for those who use new technologies to develop their professional activities in order to accept certain additional requirements to re-establish the traditional balance between the parties concerned. The justification is simple – if technology increases the capacity to accumulate, process and communicate information on others and facilitates transactions and administrative operations, it is essential that it should also be configured and used to ensure that data subjects, whether as citizens or consumers, enjoy a proportionate benefit from these advances.

Several recent provisions have drawn on the proportionality requirement to oblige those who use technologies to make them available for users to enforce their interests and rights.

One example is European Directive 2001/31/EC (the "E-Commerce Directive"), which includes electronic anti-spamming provisions. Similarly, Article 5.3 of Directive 2002/58/EC on privacy and electronic communications even includes the requirement that "(...) *the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information* (...) *and is offered the right to refuse such processing* (...)". Sub-

4. Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways, available on the Council of Europe site. See also Recommendation 3/97 of the so-called Article 29 Group: Anonymity on the Internet, and the opinion of the Belgian privacy commission on electronic commerce (No. 34/2000 of 22 November 2000, available on the commission's site: http://www.privacy.fgov.be), which points out that there are ways of authenticating the senders of messages without necessarily requiring them to identify themselves.
5. See the recommendation of the French national data processing commission that access to commercial sites should always be possible without prior identification: M GEORGES (2000). "Relevons les défis de la protection des données à caractère personnel: l' Internet et la CNIL". In: *Commerce électronique-Marketing et vie privée*. Paris, p.71 and 72.
6. Requirements could be laid down for the services provided and concerning confidentiality, as is proposed for electronic signatures. Official approval of an anonymiser would indicate that the requirements were being observed. Such official approval might be voluntary rather than obligatory, as in the case of quality labels.

scribers' right, under Article 8.1, "via a simple means, free of charge, to eliminate the presentation of the calling-line identification on a per-call basis (...) and on a per-line basis" is another potentially valuable approach if the notion of "calling line" is extended to various Internet applications, such as web services and email.[7] This implies a related obligation for the service provider to offer users the options of refusing to accept unidentified calls or preventing their identification (Articles 8.2 and 8.3).

10. Legislations called "Freedom of Information" introduce a similar right to transparency vis-à-vis government by adding further information that the latter is obliged to supply. A welcome development in the United Kingdom is the recent introduction of a public service guarantee for data handling.[8] A Swedish commission[9] has recently recommended legislation that would entitle citizens to monitor their cases electronically from start to finish, including their archiving, and oblige the authorities to adopt a good public access structure, to make it easier for individuals to identify and locate specific documents. There is even draft legislation that would make it possible, one way or another, to link any official documents on which decisions were based to other documents on the case. In other words, a public service that has become more efficient thanks to new technology must also be more transparent and accessible to citizens. Citizens' right of access extends beyond the documents directly concerning them to include the regulations on which a decision was based.

11. **It is even possible to imagine that certain of the rights associated with data protection, such as the right to information, the rights of access and rectification and the right of appeal, might soon be enforceable electronically**. Many applications could be proposed:

- it should be possible to apply data subjects' right to information at any time through a simple click (or more generally a simple electronic and immediate action) offering access to a privacy policy, which should be as detailed and complete as the greatly reduced cost of electronic dissemination allows. Such a step must be anonymous as far as the page server is concerned, to avoid any risk of creating files on "privacy concerned" users. In addition, in the case of sites that have been awarded quality labels, it should be obligatory to provide a hyperlink from the label symbol to the site of the body that awarded the label. The same would apply to the declaration of the file controller to the supervisory authority. A hyperlink would be installed between an unavoidable page of any site processing personal data and that of the relevant supervisory authority. Finally, consideration might be given to the automatic signalling of any site located in a country offering inadequate protection;
- in the future, data subjects must be able to exercise their right of access using an electronic signature. It would be obligatory to structure files so that the right of access was easy to apply. Additional information, such as the origin of documents and a list of third parties to whom certain data had been supplied, should be systematically available. As noted earlier,[10] increasingly, the personal data accumulated by the vast public and private networks are no longer collected for one or more clearly defined purpose but are stored in the network for future uses that only emerge as new processing opportunities or previously unidentified needs arise. In such circumstances, data subjects must have access to documentation describing the data flows within the network, the data concerned and the various users – a sort of data registry;[11]

7. Note the link between these provisions and the anonymity principle.
8. A Public Service Guarantee For Data Handling: now available for implementation in public bodies. This sets out people's rights about how their personal data is handled by public authorities and the standards they can expect public organisations to adhere to. http://www.dca.gov.uk/foi/sharing/psguarantees/data.htm#2
9. P. SEIPEL (2004). "Information System Quality as a Legal Concern". In: U. GASSER (ed.). *Information Quality Regulation: Foundations, Perspectives and Applications*. Nomos Verlagsgesellschaft. P. 248. See also the Swedish commission report by P. SEIPEL (2002). *Law and Information Technology: Swedish Views*. Swedish Government Official Reports, SOU. P. 112.
10. See paragraph 3.
11. This idea is the subject of two recent Belgian laws that require the establishment of sectoral committees for the networks linked to the National Register (Act of 8 August 1983 establishing a national register of persons, as amended by the Act of 25 March 2003, MB. 28 March 2003, art.12§1) and to the commercial registration authority (Banque Carrefour des entreprises) (Act of 16 January 2003 establishing the authority, MB. 5 February. 2003, article 19§4).

- it should be possible to exercise the rights of rectification and/or challenge on-line to an authority with a clearly defined status responsible for considering or maintaining a list of complaints;
- the right of appeal should also benefit from the possibility of on-line referral, exchange of parties' submissions and other documentation, decisions and mediation proposals;
- finally, when individuals concerned wish to challenge decisions taken automatically or notified via a network (such as a refusal to grant a building permit following a so-called e-government procedure), they should be entitled to information, via the same channel, on the logic underlying the decision. For example, in the public sector[12] citizens should have the right to test anonymously any decision-making packages or expert systems that might be used. This might apply to software for the automatic calculation of taxes or of entitlement to grants for the rehabilitation of dwellings.

c. Third principle: The principle of encouraging technological approaches compatible with or improving the situation of legally protected persons

12. Recommendation 1/99 of the so-called Article 29 Group (the EU Data Protection Working Party),[13] which is concerned with the threat to privacy posed by Internet communications software and hardware, establishes the principle that software and hardware industry products should provide the necessary tools to comply with European data protection rules. In accordance with this third principle, regulators should be granted various powers. This conclusion has been deduced from Recital 2 of Directive 95/46 on Data Protection which asserts that the information systems and products must be at the service of society and individuals.

For example, regulators should be able to intervene in response to technological developments presenting major risks. The so-called **precautionary principle**, which is well established in environmental law, could also apply to data protection. The precautionary principle may require telecommunications terminal equipment (including software) to adopt the most protective parameters as the default option to ensure that those concerned are not, by default, exposed to various risks of which they are unaware and which they cannot assess.

Similarly, in accordance with the principle of reciprocal benefits, it is appropriate and not unreasonable to equip telecommunications terminal equipment with web logs, as is the case with server-type software used by on-line undertakings and government departments. This would enable users to monitor persons who have accessed their equipment and, where appropriate, identify the main characteristics of the information transferred.

13. This principle can be illustrated by a provision of the EU Directive on privacy and electronic communications. Article 14 states that where required, the Commission may adopt measures to ensure that terminal equipment is compatible with data protection rules. In other words, standardising terminal equipment is another, admittedly subsidiary, way of protecting personal data from the risks of unlawful processing – risks that have been created by all these new technological options. Going further, it is necessary to prohibit the so-called privacy killing technologies,[14] in accordance with the security principle enshrined in Article 7 of Council of Europe Convention 108. The obligation to introduce appropriate technical and organisational measures to counter threats to data privacy will require site managers to make sure that messages exchanged remain confidential, indicate clearly what data is being transmitted, whether automatically or by hyperlink, as is the case with cybermarketing companies, and make it easy to block such transmission.

This security obligation will also require those who process personal data to opt for the most appropriate technology for minimising or reducing the threat to privacy. This requirement clearly has an influence on the design of

12. The same principle applies to private decision makers, subject to the legitimate interests of the file controller (particularly relating to business confidentiality, which could limit the duty to clarify the underlying logic).
13. Art. 29 W.G. Recommendation on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware.
14. Expression used by J.M. DINANT in "Law and Technology Convergence in the Data Protection Field?". In: I. WALDEN; J. HORNE (2002). *E-commerce Law and Practice in Europe*. Cambridge: Woodhead Publishers Ld. Chapter 8.2.

smart cards, particularly multifunctional cards,[15] such as identity cards. Another example of the application of this principle concerns the structuring of medical files at various levels, as recommended by the Council of Europe.

14. **It might be possible to go further by recommending, as the EU Commission has done very recently (May 2nd 2007), the development of privacy enhancing technologies, that is tools or systems that take more account of data subjects' rights**. Clearly, the development of these technologies will depend on the free play of the market, but the state must play an active part in encouraging privacy compliant and privacy enhancing products by subsidising their research and development, establishing equivalent voluntary certification and accreditation systems and publicising their quality labels, and ensuring that products considered necessary for data protection are available at affordable prices.

d. Fourth principle: The principle of full user control of terminal equipment

15. The justification for this principle is obvious. Since these terminals can enable others to monitor our actions and behaviour, or simply locate us, they must function transparently and under our control. Article 5.3 of Directive 2002/58/EC, cited above, offers a first illustration of this point. Those concerned must be informed of any remote access to their terminals, via cookies, spyware or whatever, and be able to take easy and effective countermeasures, free of charge. Directive 2002/58/EC also establishes the rule that users of calling and connected lines can prevent the presentation of the calling line identification.

Going beyond these examples, we would also argue that **all terminal equipment should be configured to ensure that owners and users are fully informed of any data flows entering and leaving, so that they can then take any appropriate action**. Similarly, as is already the case under some legislation, possession of a smart card should be accompanied by the possibility of read access to the data stored on the card.

16. User control also means that individuals can decide to deactivate their terminals once and for all, and at any time. This is important as far as Radio Frequency Identifiers (RFIDs) are concerned. Data subjects must be able to rely on third parties[16] that vouch that such technical means of remote identification have been fully deactivated.

Users may well apply this principle to firms that are not necessarily covered by traditional data protection rules because they are not responsible for data processing. Examples include suppliers of terminal equipment and many forms of browser software that can be incorporated into terminals to facilitate the reception, processing and transmission of electronic communications.

The principle also applies to public and private standard setting bodies concerned with the configuration of such material and equipment.

17. **The key point is that the products supplied to users should not be configured in such a way that they can be used, whether by third parties or the producers themselves**, for illicit purposes. This can be illustrated by a number of examples:

- a comparison of browsers available on the market shows that chattering between them goes well beyond what is strictly necessary to establish communication;[17]
- browsers differ greatly in how they receive, eliminate and prevent the sending of cookies, which means that the opportunities for inappropriate processing will also vary from one browser to another. However, blocking pop-up windows or the systematic communication of references to articles read on-line or of keywords entered on search engines is apparently impossible, at least in a simple way, on the default browsers installed

15. On the privacy compliant design of multi-application cards, see E. KEULEERS; J.M. DINANT (2004). "Data protection: multi-application smart cards. The use of global unique identifiers for cross-profiling purposes". Part 2: "Towards a privacy enhancing smart card engineering". In: *Computer Law and Security Report*. Oxford: Elsevier. Vol. 20, nº 1, pp. 22-28.
16. Clearly this refers to accreditation arrangements such as those already described in paragraph 15 (joint regulation) or to approval issued by the authorities to certain undertakings (public regulation).
17. See Jean-Marc DINANT (Winter 2001). "Le visiteur visité". *Lex Electronica*. Vol. 6, nº 2

on the majority of the hundreds of millions of personal computers.
- Attention should also be drawn to the use of unique identifiers and spyware by suppliers of browser tools and communication software.

18. **More generally, terminal equipment should function transparently so that users can have full control of data sent and received. For example, they should be able to establish, without fuss, the precise extent of chattering on their computers, what files have been received, their purpose and who sent or received them. From that standpoint, web logs appear to be an appropriate tool that is relatively easy to introduce**.

19. In addition to the users' right to be informed of data flows entering, there is the question of whether persons are entitled to require third parties to secure authorisation to penetrate their "virtual home". Of relevance here is the Council of Europe Convention on Cybercrime, particularly articles 2 (illegal access)[18] and 3 (illegal interception).[19] In this case, the identification or identifiability of persons taking part in telecommunications is not a precondition for the Convention's application. Similarly, unauthorised access to a computer system is not confined to hacking into major systems operated by banks or government departments but also concerns non-authorised access to telecommunications terminals, represented in the current state of the art by computers.[20]

In other words, we maintain that placing an identifying number in a telecommunications terminal or simply accessing this number or some other terminal identifier generally constitutes unauthorised access. In such a legal context, there can be no question of assessing the proportionality of such actions. Authorisation remains a positive act that is quite distinct from any acceptance that might be inferred from silence or a failure to object.

It cannot therefore be assumed, as DoubleClick did,[21] that simply by failing to activate a cookie suppressor users have authorised all and sundry to install this type of information on their terminals.

e. The principle that users of certain information systems should benefit from consumer protection legislation

20. **The routine use of information and communication technologies, formerly confined to major undertakings, and the rapid development of electronic commerce that has multiplied the number of on-line services have led to a more consumerist approach to privacy**. Web surfers increasingly view infringements of their privacy –spamming, profiling, differential charging policies, refusal of access to certain services and so on – from the standpoint of consumers of these new services.

Thus, in the United States the first hesitant steps towards legislation on data protection in the private sector focussed on on-line consumer protection. Reference has already been made to Californian legislation[22] but we should also bear in mind the 1995 Consumer Privacy Act

18. Article 2 - Illegal access: Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.
19. Article 3 - Illegal interception: Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.
20. See, in this context, the excellent article by THIERRY LEONARD, "E-commerce et protection des données à caractère personnel: Quelques considérations sur la licéité des pratiques nouvelles de marketing sur internet" on http://www.droit.fundp.ac.be/Textes/Leonard1.pdf
21. Following a class action brought against it several years ago in the United States, DoubleClick's practice is now to send all non-identified terminals an initial non-residual and non-identifying cookie named "accept cookies". If the cookie is returned, DoubleClick assumes that the terminal accepts cookies and sends an identifying cookie that remains in place for about ten years (previously thirty). If the cookie is not returned, DoubleClick will indefinitely send the cookie requesting authorisation. An opt-out is available that enables informed users to store a cookie that signifies that they do not accept them.

and, more recently, the 2000 declaration of the Federal Trade Commission,[23] which emphasised the need for privacy legislation to protect on-line consumers. In Europe as in America, measures to combat spamming are concerned with both consumers' economic interests and data subjects' privacy.

21. **This convergence between consumers' economic interests and citizens' freedoms opens up interesting prospects**. It suggests that the right to resort to certain forms of collective action, which is already recognised in the consumer protection field, should be extended to privacy matters. Such an entitlement to "class actions" is particularly relevant in an area where it is often difficult to assess the detriment suffered by data subjects and where the low level of damages awarded is a disincentive to individual actions.

In addition, many other aspects of consumer law could usefully be applied to data protection. Examples are the obligations to provide information and advice, which could be imposed on operators offering services that essentially involve the management or supply of personal data, such as Internet access providers and personal database servers (case-law databases, search engines and so on), the law governing general contractual conditions (applicable to privacy policy) and measures to combat unfair commercial practices and competition.

Finally, providing personal data as a condition of access to a site or an on-line service could be viewed not merely from the standpoint of data protection legislation – does the user's consent meet the necessary requirements and is it sufficient to legitimise the processing in question? – but also that of consumer law, if only in terms of unfair practices in obtaining consent or the major detriment arising from the imbalance between the value of the data secured and that of the services supplied.

Another avenue to be explored is whether consumer product liability for terminals and software can be extended beyond any physical and financial harm caused to include infringements of data protection requirements. How far is the supplier of browser software whose use leads to breaches of privacy objectively liable for data infringements by third parties?

Conclusions

22. The advent of the Internet has created a need for a third generation of data protection regulations. It is not a question of turning one's back on the first two generations but of providing an additional level of protection, while leaving unaltered the measures already introduced. The first generation was mainly based on the nature of the data, namely whether it was sensitive and concerned individuals' private domain. Informational self-determination was then equated with banning the processing of such data, and was encapsulated in Article 8 of the European Convention on Human Rights. The second generation was concerned not just with protecting personal data, but also with the way in which its processing could modify the balance of power between information processors and the subjects of that processing. Informational self-determination was thus extended to adjusting this balance by ensuring that such processing remained transparent and restricting the right to process data about others. This was the origin of Convention No. 108. It has many emulators and has amply justified its existence.

23. **The emerging third generation, which we hope will be rapidly adopted, is characterised by its recognition of the technology itself**. The use of new technologies multiplies the amount of data and the individuals capable of accessing it, increases the power of those who collect and process it, and bridges frontiers. A further factor to be taken into account is the complexity and opacity of this technology. A third party – be it the terminal or the network – now intervenes between individual and data controller. Informational self-determination calls for a measure of control over this third party.

22. See paragraph 12.
23. See the report to Congress "Privacy Online: Fair Information Practices" May 2000, available on the FTC site: http://www.ftc.gov/os/2000/05/index.htm. In the United States, the FTC, which is very active in the consumer protection field, has played a key role in protecting citizens' privacy.

How should this control be exercised? The following suggestions do not exhaust the subject:

- "The answer to the machine is in the machine" according to Clarke,[24] in connection with the problems the information society poses for copyright. It may also suggest ways of tackling the threats that same society poses for privacy. As has already been seen, the principle of reciprocal benefits and the promotion of "privacy minded" technological approaches can help those concerned to exercise closer control over the circulation and use of their personal information.
- This optimism has its limits. Although these technologies may contribute to what some call user empowerment, there is a risk that the individuals concerned will be left to face data controllers unaided. In reality, the technology is not neutral: although it is widely on offer to citizens, it is still indirectly financed by the businesses and official agencies and departments that pay the computer servers. Inevitably, the latter are likely to be more attentive to data controllers' interests than to those of data subjects. So-called privacy protection technology transforms or could transform the relationship between individuals and their own personal data into a property relationship that, thanks to the new technologies, becomes negotiable. It therefore needs to be stressed that informational self-determination is a personal freedom that is absolutely not open to negotiation and that society has a duty to fix certain limits to the right to use these data.
- This focus on the technological tools must also extend to new players outside the ambit of second generation legislation, namely communication services and terminal equipment suppliers. Their role is critical to any attempts to enable the users of new information society services to monitor data entering and leaving the system, as well as the data tracks they offer to networks and their possible use. Consideration must be given to establishing strict liability for the supply of privacy compliant equipment and services.

24. **What exactly does this liability of terminal equipment producers and communication services providers mean?** In our opinion, Internet access providers, and mobile and other telephone operators, are responsible for informing the public of the risks attached to the use of their networks, reporting privacy-threatening technologies and offering access to appropriate privacy-friendly applications. These access providers have a key role as they act as gatekeepers between users and the network. They are therefore asked[25] to "inform users about technical means which they may lawfully use to reduce security risks to data and communications", to "use appropriate procedures and available technologies, preferably those which have been certified, to protect the privacy of the people concerned (...), especially by ensuring data integrity and confidentiality as well as physical and logical security of the network" and to inform Internet users of ways of "using its services and paying for them in an anonymous way". Subscribers should be offered a hotline enabling them to report privacy violations and providers should subscribe to a code of conduct requiring them to block access to sites that fail to meet data protection requirements, no matter where the site is located.

The second target is made up of equipment and software manufacturers and developers, and those responsible for drawing up technical standards and protocols used in the transmission of network information. They should ensure that their products or standards:[26]

- comply with the law, for example by ensuring that Internet browsers transmit the minimum information necessary for connection and adopting appropriate security measures;
- facilitate the application of the principles outlined in Part II, for example to allow users direct access to their personal data and a right of automatic objection, particularly through the use of web logs;
- raise the level of protection of personal data.

25. Perhaps, in the same line, we must enlarge the scope of the protection as regards the data covered by Privacy legislations. New technology makes it increas-

24. C. CLARKE (1996). "The answer to the machine is in the machine". In: B. HUGENHOLTZ (ed.). *The Future of Copyright in a Digital Environment*. Kluwer. P. 139 ff.
25. Council of Europe Recommendation R (99) 5, III, 1, 2 and 4.
26. See the Belgian Commission opinion no. 34/2000 on e-commerce and data protection.

ingly possible to process data relating to individuals not, as was traditionally the case, through data relating to their legal identity, such as name or address, but via an anchor point or even an object (so-called ambient intelligence) associated with it. Data generated by cookies, as well as those generated by RFID tags embedded in clothes or in products, are not necessarily referring to an individual but since they permit to contact and even to take decisions vis-à-vis a person, the person behind the terminal in the case of cookies, the person having the clothes or the products in the case of RFID, must be subject to certain protection.

26. Terminals, in the broad sense, must become totally transparent technological tools for those who have and use them. Moreover, in many cases they actually belong to the individuals concerned and may be seen as part of their home. Any intrusions into their privacy must be treated like any other intrusion.

The opacity and complexity of sophisticated information systems to which persons submit data call for surplus information that is no longer focused solely on the processing itself or individual characteristics, but rather on the overall functioning of the information system and its ability to generate a vast quantity of information, present and future. Hence the need to document data (origin, users, logical justification), describe the various information flows and lay down rules governing how decisions are taken, who has access and how it is monitored.

Hitherto, the data protection authorities have traditionally paid no attention to technological tools. They rarely employ computer specialists or penetrate the inner sanctums of those who decide what technological developments will take place and how products will be configured. Just as European states have demanded the establishment of a Governmental Advisory Committee (GCA) to the ICANN, a private body responsible for managing Internet domain names and addresses, it might equally be necessary to propose or even insist on a Data Protection Advisory Committee to ICANN, W3C (World Wide Web Consortium) and the IETF (Internet Engineering Task Force). It is necessary to make the electronic communications sector fully aware of the importance of data protection.

27. To summarise, I would like to stress the two main following needs:

- the need to supply individuals with all they need to understand and control their computer environment, particularly where it penetrates their homes. They must be given control of any tools whose use reveals them to others;
- the need to give society the tools to control technological developments that could otherwise threaten the survival of our individual and collective liberties.

Highway legislation imposes certain rules on users not just to reduce accidents but also to strike a satisfactory balance between the rights and obligations of different road users, with the courts being inclined to offer particular protection to the most vulnerable among them. This necessitates not just a highway code but also specific legislation on the road network itself and the vehicles permitted to use it, which are subject to certain mandatory standards.

On the information highways, there is no legislation laying down operating rules for telecommunications to protect users' privacy or requirements to ensure that telecommunications terminals that allow users to travel on these highways operate fairly and transparently.

Only by applying traditional data protection principles to these new technologies, which are implicit but unavoidable components of all telecommunications, can computerisation lead to a democratic information society, bringing general progress for all.

Recommended reference

POULLET, Yves; DINANT, Jean-Marc (2007). "Towards new Data Protection Principles in a new ICT environment". In: "III Conference on Internet, Law and Politics (ILP). New outlooks" [on-line monograph]. *IDP. Revista de Internet, Derecho y Política*. No. 5. UOC. [Date of consultation: dd/mm/yy].

<http://www.uoc.edu/idp/5/dt/eng/poullet_dinant.pdf>

ISSN 1699-8154

About the authors

Yves Poullet
Yves.poullet@fundp.ac.be

Professor at the Faculty of Law of Namur and Liège (Belgium). Licentiate in Philosophy and Doctor of Law. Director of the "Centre de Recherche Informatique et Droit" at Les Facultés Universitaires Notre-Dame de la Paix de Namur (Belgium). Professor of Law, especially in the teaching of "Freedoms and the Information Society", and Dean of the Faculty of Law at FUNDP. He is also a professor at the University of Liege.

Jean-Marc Dinant
Jean-marc.dinant@fundp.ac.be

Lecturer at the Computer Science Institute and CRID (University of Namur)